AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY

CYBERSPACE PROTECTION AND THEORY

by

Marion Grant, Major, United States Air Force

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Roger Philipsek

Maxwell Air Force Base, Alabama

06 April 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Abstract

This paper provides Air Force Space Command (AFSPC) suggestions on cyber protection and theory. First, AFSPC must instill a sense of cybermindedness to all network-based resource users. This includes daily actions and in-processing/out-processing events. Secondly, AFSPC must lead the charge to establish a common naming convention for all cyber resources, thus promoting a familiarity with capabilities as in the air, land, sea, and space environments. Next, AFSPC must conduct a study leading to the formation of a cyber standard model, similar to the standard atmosphere model used in aviation. Specifically, AFSPC needs to study the establishment of a test and evaluation standard model for cyber networks. Finally, AFSPC must use enterprise wide network traffic generation as a means of tactical deception for cyber protection. This concept will hide true network traffic in the midst of scheduled, characterized, realistic, and random network data, and is analogous to the concept of chaff's effect on radar cross section. These recommendations are based on years of experience in network operations, flight and information operations systems test, and the thoughts of flight test and network security engineers. Adherence to these recommendations will provide AFSPC a decisive edge in cyber operations.

1. Introduction

Motivation and Purpose

This paper provides answers to AFSPC on the subjects of cyberspace protection and cyberspace theory. Specifically, this paper will answer the Air University Information Management System (AURIMS) AFSPC Academic Year 2010 submitted questions of cyberspace protection and cyberspace theory. On the subject of cyberspace protection, AFSPC has requested "a cyberspace protection strategy that informs a list of viable protection options"[1]. The cyberspace theory topic looks to current military theory to provide "AFSPC with observations and recommendations"[2]. The research methodology used to address these questions is that of problem/solution.

Scope

The different options within this paper are presented as independent views on the two theories mentioned above. Although each of the options is autonomous, the true benefit for AFSPC is the synergy between the options. Linkages between the different options are highlighted as appropriate. The options presented are to:

- Increase the cybermindedness of the general public
- Promote common terminology within cyber by use of a standard naming convention for cyber capabilities
- Create a cyber standard model, analogous to aviation's standard model, for use in cyber test and evaluation.
- Employ tactical deception as a means of data protection in cyber networks

This research is limited in the following ways:

- Although there are suggestions presented in this work on the data collection needed, the exact means to do so are not part of this paper

Organization of Thesis

Chapter two probes the idea behind instilling a cybermindedness into the American culture, much the same as the early days of the USAF. This is the most important step in the protection of AFSPC cyber resources. Chapter three outlines the need for a cyber standard naming convention, which is complimentary to the instilling of cybermindedness. Chapter four, building upon the previous chapter, presents the case for a cyber standard model (analogous to the aviation standard atmosphere model) that provides the necessary structure, discipline, and data for use in the tactical deception topic. Chapter five, the final chapter, presents the tactical deception method needed for the protection of AFSPC cyber resources.

2. Cybermindedness

AFSPC must instill cybermindedness into the USAF's cyber users. This cybermindedness will serve as the means to make USAF users aware of cyber assets (specifically network-based assets) beyond that of a tool that edits documents, displays slides, and sends emails. It is only when users understand, in simple and socially accepted terms, that the use of network-based resources is a privilege, that the importance of the resource is realized. USAF leadership has stated that all users within cyber "must own the problem"[3] This example is a start, but I suggest that a visit to the early days of USAF history provides a template for AFSPC.

During the earliest days of United States military aviation, its founders decided that the best way to achieve an independent Air Force was to push the importance of strategic bombardment theory. Their beliefs in strategic bombardment theory, and the importance of the airplane, were influenced by the early writings of General Jan Smuts, who proclaimed the below in the Smuts Report.

> "…and the day may not be far off when aerial operations with their devastation of enemy lands and destruction of industrial and populous centers on a vast scale may become the principal operations of war, to which the older forms of military and naval operations may become secondary and subordinate."[4]

General Arnold understood that society's adoption of the airplane would prove beneficial to the early USAF as it tried to separate from the Army. To that end, General Arnold worked with the defense industry to indoctrinate the public to aviation, culminating with his writing of children's stories "to create a favorable image of the "airman" for America's youth."[5] This tactic worked, as junior aviation clubs soared in memberships.[6]

Additionally, other civilian and military leaders used their influence and knowledge of aviation to introduce the American society to the concept of flight. Specifically, Thomas Edison

wrote of a gas bombing that would spell doomsday for any large city, and General Kenney staged mock bombings of American cities to stress the need for the Air Force and its mission[7]. The same type of vigor and enthusiasm must happen within cyber, with the primary focus on protection of assets.

AFPSC should initiate a cybermindedness indoctrination campaign for the American people. By this, I do not imply a "brainwashing" of the American people for the cyberspace cause, nor do I propose using this campaign for the purposes of creating a separate cyber force. The American people must simply achieve a basic understanding of how to protect themselves in cyberspace. This point is reinforced by a SANS institute news article entitled "Jargon Hinders Everyday Users' Understanding of Cyber Security (February 19, 2010)", which reported on a similar topic, and is included below.

> "Computer experts meeting in Belgium last week discussed problems in cyber security culture that stand in the way of helping regular users protect themselves and their computers. Jargon lends a "mystique" to security, which results in a lack of clarity and among some, a sense of superiority over those who are not well versed in the technical aspects of cyber security. Cyber security language needs to be simplified and users need to be told why they are being asked to do things like create string passwords and keep them secret, or install security software; the risks of not taking cyber security precautions need to be made clear and real. Education about cyber security needs to be informative and interesting and created to target various age groups and audiences."[8]

Further evidence is found in a Zogby poll on cyber security and education.

> "A new Zogby poll on cyber security and education reveals that, while 90-percent of administrators believe it's important to teach kids basic Web safety, a vast majority offer no such lessons. The study, commissioned by the National Cyber Security Alliance (NCSA) and Microsoft, found that only 27-percent of teachers offered any instruction on safe social networking, and less than 20-percent broached the topics of avoiding fraud and creating a secure password.
>
> Michael Kaiser, executive director of the NCSA, told The Hill, "The study illuminates that there is no cohesive effort to provide young

> people the education they need to safely and securely navigate the digital age and prepare them as digital citizens and employees." He also pointed out that President Obama has specifically called for such educational programs, and that the time to act is now.
>
> Most high schools still offer basic technology and computer classes, most of which are focused on skills far below the students' existing capabilities. We're with Kaiser; now is the time to update these classes with lessons applicable to the 21st century, and to stop worrying about teaching them to use Word."[9]

The Department of Homeland Security (DHS) understands the facts arising from these and similar statements, as it has implemented the National Cybersecurity Awareness Campaign Challenge, which "is working with many organizations, both individually and through the National Cyber Security Alliance, to find ways of raising public awareness of cybersecurity."[10] The challenge has eleven focus areas, and has the grand purpose to invoke "competition that will gather and share publicly the best, most creative ideas for making the public more cyber secure, cyber smart, and cyber assured."[11] The most important part of the eleven focus areas is the message. This is the communication that DHS is trying to place into the hearts and minds of all cyber users.

The attitude of perceived elitism and the lack of the appropriate level of communication, described above, do not promote people learning the most that they can about cyberspace, especially network security. This is where AFSPC can train all users that they are stewards of the cyber enterprise, and that as a cyber stewards they have the responsibility for the defense of the enterprise at work and, more importantly, at home. Users must understand that actions taken at home on personal computers, laptops, and mobile devices have a direct effect on the security of the work cyber environment. The above is reinforced by the "United States Air Force Blueprint for Cyberspace" document, dated 02 November 2009, in which it is stated, "A cultural

change is also critical in the USAF operation and defense of the AF-GIG. Every USAF airman, government civilian, and contract partner must become a cyber defender."[12]

The United States Air Force Blueprint for Cyberspace prescribes the following for the protection of USAF networks.

> "Airmen have a critical role in defending the USAF networks. They can significantly decrease the adversary's access to the USAF networks by:
>
> - Not opening attachments or click on links unless the email is digitally signed, or directly verifying the source directly
> - Not connecting any hardware or download any software, applications, music or information onto our networks without approval
> - Encrypting sensitive but unclassified and/or mission critical information
> - Installing the free Department of Defense anti-virus software on home computers."[13]

Expanding upon this work, it is suggested that AFSPC perform the actions listed in Table 1 Cybermindedness Actions. Each action is listed with the benefit that it would provide to the cybermindedness objective.

Cybermindedness Action Needed	Cybermindedness Benefit Gained
Issue home use anti-virus software during in-processing and out-processing; require notification of install and configuration of automatic update during in-processing.	1. Protects user's home computing environment 2. Protects file transfers between home and work 3. Promotes cyber stewardship and network security
Expand Information Assurance and Information Protection training to incorporate: 1. Basic knowledge of networks and networking 2. Basic concept of ports, services, and data transit 3. Concept of firewalls (home use program)	1. All users at a common level of understanding 2. Teaches users how to protect themselves 3. Hinders the accidental or malicious data leakage from home networks. Ex. Teach users that to connect (port 80 or 443) to a website, you ***do not*** have to allow (port 80 or 443) into your home network.
Provide help desk support for home use protection	1. Users are more likely to use the program if they have support for any types of questions they have.
Teach the concept of "less is more" for home	1. Less services running = less avenues of attack Ex. If a home machine only surfs the web and prints via a USB printer then there exists no need for the Windows NetBIOS (file sharing) services. Likewise, this same computer would not need to allow Remote Registry (core of Windows operating system) access or IPv6 (next version of Internet Protocol).
Teach the concept of "less is more" for the enterprise	1. Same concept as above, yet on enterprise level. 2. Air Force should minimize to thin client architecture, with PCs as the exception. (As a thought experiment—Do you need a full PC or just access to office automation resources?)

Table 1 Cybermindedness Actions

Conclusion

The actions presented above are only a start at protecting the assets of the cyber enterprise, yet they are still able to contribute to immediate security of the enterprise. A user of cyber resources should be as familiar with basic cyber defenses as a military member is familiar with the term “about face”. To further promote that familiarity AFSPC must institute standardization within cyber. The first step in this is to implement a standard naming convention within the domain.

3. A Cyber Standard Naming Convention

USAF cyber users must be made aware of the need to protect both home and work related cyber resources. This will only come about once the mystifying and perceived elitist aspects of cyber terminology and discussion disappear. Not only must this occur with the standard users, but also with the operators of the network.

Conventional wisdom states that to properly defend, one must understand how the offense works. The offensive in cyber, best characterized through hackers of computer networks, generally has capabilities that fall into five groups. These groups are tools that perform denial of service (DoS), privilege escalation, propagate worms or viruses, perform man-in-the-middle actions, or log hardware or network information. These tools work at various levels of and on different types of cyber resources. The levels and types are application, operating system, protocol, and service. Finally, each of these tools can be further categorized into which type of cyber resource they target. For simplicity, these types of resources are described as Windows based, non-Windows based, and infrastructure based.

To aid in the discussion of cyber capabilities, AFSPC should adopt similar naming conventions used within the air domain. As air operators understand the term GBU-31 to be a

Guided Bomb Unit 31, or Joint Direct Attack Munition, so must cyber operators have such a familiarity with available resources. Again, this provides a means of communicating, in simple terms, to the users and commanders the nature of the real threat. Without such a naming convention, confusion will continue, and the real meaning of the message will be lost on the audience. To illustrate, an example is appropriate.

Referencing USAF doctrine on Information Operations (AFDD 2-5) and general practice within the cyber community, one would have to describe a scenario in which the base network is under network attack from a denial of service tool from an outside source as the following. "The A6 states that the base is currently under NetA from a hostile outside source. The source is using a distributed denial of service application, called Mag_tran 1.1, that is causing the base CISCO routers to slow down. This attack has impacted mission readiness by thirty percent. There is no evidence of successful Windows administrator or Unix/LINUX root access tools used as of yet. Base and Air Force Network Defenders are using Wireshark and tcpdump network traffic sniffers to monitor the situation."

The above hypothetical scenario makes sense to those who are in constant contact with the cyber domain, specifically the network warfare operations potion, yet can easily become confusing to those who are not as well versed in the terminology. Using slightly less technical terms, the A6 can relay the same message without causing the proverbial "deer in the headlights look" most commonly associated with this type of information. A proposed solution to the jargon used above is included in the below table of names.

Category	Type	Desgination	Target Infrastructure, Non-Windows-based sytems, Windows Based Systems
Cyber Weapon (CW)	Denial of Service (includes distributed)	DCW	DCW-I, DCW-N, DCW-W
	Automated (Virus and Worm)	ACW	ACW-N, ACW-W
	Privelege Escalation	PCW	PCW-I, PCW-N, PCW-W
Cyber Enabler (CE)	Logging (man-in-the-middle, sniffers, and loggers)	LCE	LCE-I, LCE-N, LCE-W

Table 2 Cyber Naming Convention

Referencing USAF doctrine on Information Operations (AFDD 2-5) and now using the above table, one would now describe a scenario in which the base network is under network attack from a denial of service tool from an outside source as the following. (NOTE: Table 2 Cyber Naming Convention uses the suffixes I for Infrastructure, N for non-Windows based operating systems, and W for Windows based operating systems.) "The A6 states that the base is currently under NetA from a hostile outside source. The source is using a DCW, specifically a DCW-I, that has impacted mission readiness by thirty percent. There is no evidence of successful use of PCWs as of yet. Base and Air Force and Network Defenders are using LCEs to monitor the situation. Specifics can be addressed in a side meeting."

Conclusion

A standard way of referencing information within the cyber community is fundamental to any further progress within the cyber domain. Once established, it is then best for AFSPC to characterize and understand the cyber resources that are under its control. To accomplish this, AFSPC should institute a cyber standard model for network-based operations within all Air Force networks.

4. A Cyber Standard Model

Individuals involved within the cyber domain often define new terminology based on the perceived unique aspects of cyber without first considering previous work in other domains. The cyber industry recognizes this as a problem.[14] They know that cyber professionals do not all speak the same language, and that the problem resonates beyond the military.[15] Industry also understands that standardization presents problems, and that there is "no such thing as a standard network".[16] One can argue that these items are natural parts of the evolutionary process of new technologies, techniques, or doctrinal changes.[17] However, in continuing down this path, issues in integration with existing air, ground, sea, and space operations will persist.

Cyberspace, according to the Department of Defense, is "the notional environment in which digitized information is communicated over computer networks."[18] This chapter focuses on the part of cyberspace needed for computer networks used in system test and evaluation (T&E). It begins by describing the nature of the aeronautical standard model and its use in flight test. A discussion of the problems of standardization in cyber T&E by use of a short hypothetical scenario follows. This chapter concludes by calling for the establishment of a cyber standard model.

"The performance of any flying machine will be greatly influenced by the atmosphere in which it is flying."[19] The Earth's atmosphere is dynamic in nature. That fact, the "new born missile industry", and the "space race of the 1950's,"[20] led to the need for atmospheric characterization. Engineers from the National Aeronautics and Space Administration, the United States Air Force, and the National Oceanic and Atmospheric Administration characterized the atmosphere via air data collection and analysis.[21] The premise behind the characterization is that as altitude increases from sea level, air pressure, temperature, and density decrease.[22]

Assumptions of the characterization were that the air is dry, the air is a perfect gas, air will allows flow from high to low pressure areas, and gravitational fields decrease with altitude.[23] This premise and the assumptions resulted in a standard atmosphere model, which accounts for variations in the atmosphere, provides flight test engineers a process to normalize data from different test days and ranges, and implements a standard day (the at sea level reference point for the standard atmosphere model). The official definition of the standard atmosphere is as follows:

> "… a hypothetical vertical distribution of atmospheric temperature, pressure and density which, by international agreement, is roughly representative of year-round, midlatitude conditions. Typical usages are as a basis for pressure altimeter calibrations, aircraft performance calculations, aircraft and rocket design, ballistic tables, and meteorological diagrams. The air is assumed to obey the perfect gas law and hydrostatic equations which, taken together, relate temperature, pressure and density with geopotential. Only one standard atmosphere should be specified at a particular time and this standard atmosphere must not be subjected to amendment except at intervals of many years."[24]

The experimentation and data collection that went into the standard atmosphere model allowed man to master the air domain. Now, man seeks to master the cyber domain without a model to do so.

There are many types of cyber capabilities and techniques; yet contrary to the air domain, there exists no established model to determine performance. The standard atmosphere model allows a flight test engineer to compare air vehicle performance to a known standard even if the flight test data are collected on non-standard days and on different test ranges. Cyber T&E needs such a model.

To illustrate, let us walk through a scenario on a hypothetical cyber test range. The range consists of 100 clients, operates at 10 gigabits per second, is heterogeneous (a mixture of Windows and non-Windows operating systems), and has automated traffic generation simulating

a large business's research and development department. A developer desires to test a cyber system under test (SUT) on the range, with the purpose of determining SUT performance.

Let us now assume that the SUT meets the success criteria (minimum number of test points needed prior to evaluating a system's performance), with the exception of two test points due to a catastrophic range malfunction. At this point, all testing must continue on another cyber range. The final assumptions are that the new range has fifty percent of the first range's clients, runs at a 100 megabits per second, is homogenous (all clients are Windows based operating systems), and runs automated traffic generation based on a small business's executive department. Prudence requires regression testing of the SUT on the new range. As the regression check proceeds, the SUT fails due to perceived error in performance. Did the SUT fail or was its performance simply different on the second range? Does the developer implement fixes for the SUT based on this range, or rely on the previous range's data? What does an operator use as guidance for the SUT's performance after SUT delivery? As evidenced throughout this scenario, there exists no model to normalize data from different test locations. This is a problem.

Can one imagine such a situation in the air domain when determining air vehicle performance? Would a flight test engineer dare suggest, without first normalizing data, changing air vehicle design due to data discrepancies on separate ranges? Would airline pilots takeoff from airfields without knowing the performance of their aircraft and the density altitude? They do not consider such actions due to the standard atmosphere model that provides the means to account for atmospheric differences.

Cyber test professionals must learn from their aviation brethren, and attempt to standardize the discipline. The first step in this process is for cyber T&E to establish a standard

model to characterize the dynamic nature of the domain. Drawing on the analogies of the standard atmospheric model, cyber T&E must create a standard infrastructure model, with a standard network being the equivalent of a standard day. Flight test organizations can offer expertise from the years of experience with their standard atmosphere model. Cyber operators and cyber T&E personnel can provide the domain expertise needed to determine the unique factors of the cyber domain that would form the basis of the cyber standard model.[25] These unique factors would be analogous to the air pressure, temperature, and density of the standard atmosphere model. A cyber standard model would provide air and cyber professionals with a common terminology, and a framework to determine cyber system performance. In addition, the model would provide cyber test engineers a means to scale cyber test ranges (number of hosts, network speed, types of hosts/targets, traffic generation, etc.) based on a standard network.

To embark upon the effort of defining a standard model for cyber would require the same rigor put forth in determining the standard atmosphere model. Early theory suggests that autonomous or "bot" agents (semi-autonomous data collection applications/agents) would deploy to various networks for prolonged data collection and analysis. In addition, early theory suggests that there would be more than one type of cyber standard model based on the type of network desired for range use (logistics, personnel, maintenance, operations, etc.).[26,27] This early theory also suggests a model that is susceptible to update as needed.[28] These aspects of early theory are in-line with the standard atmosphere model. There is more than one version of the model, and necessary updates are allowed.[29,30] This position is reinforced by the contributors cited within this section, and the work of Major Repik. In his work, "Defeating Adversary Network Intelligence Efforts With Active Cyber Defense Techniques", Major Repik concluded that further work into the "characterization of each network's emanations is key", and that "these

signatures would also likely evolve over time, so determining that rate of change and periodically updating them would be required."[31]

Returning to the hypothetical cyber test range above, assuming a standard cyber model did exist, one can deal with the data discrepancies between the cyber test ranges, and adequately judge if the SUT failed its measures of performance. Cyber test engineers, armed with a tool that drives common terminology and data normalization, are now able to compare data from both ranges to the cyber standard model. At this point, the SUT's performance can accurately be stated to operators and engineers.

Conclusion

Several organizations conduct cyber T&E. These organizations create tools and reports that find use in today's operations. As cyber T&E matures, the need for a disciplined approach to domain T&E is paramount. A standard model is needed for the professionalization of cyber T&E. The aviation standard atmospheric model provides several lessons learned for cyber T&E professionals. The parameters for a cyber T&E standard model, the number of models needed, and data collect methodology for the model are beyond the scope of this paper. That said, the connection between determining those unique attributes and the next chapter of this paper are linked, as the discussion moves towards cyber protection via tactical deception in computer networks.

5. Tactical Deception for Protection

Network-centric Strategic-level Deception (NSD) is defined as "a coordinated wrapping of many small elements of misinformation and deceptive actions within a scheme across multiple computer networks."[32]

Captain Philip Erdie presented a Naval Postgraduate School thesis, "Network-Centric Strategic-Level Deception" that covered NSD. He examined the "value of network-centric

strategic-level deception operations, which, if conducted during all phases of conflict, and in particular, during peacetime, would strengthen national C4I assets, support geo-political and military operations, and potentially deter future conflict".[33] His research was based on the lessons learned from the 1973 Yom Kippur War, in which the Egyptians used over one hundred and fifty deceptive actions to aid their attack, and the London Control System (established by Prime Minister Winston Churchill) that was primarily focused on the strategic level of deception when applied to the German adversary.[34] Captain Erdie asserts that the primary purpose of Network Strategic Deception (NSD) "…is to influence adversarial decision makers before conflict occurs."[35]

Captain Erdie believed that NSD allows for "influencing of adversarial actions and creating opportunities for tactical gain or diplomatic leverage; …sustained network access even if adversarial sensors monitor network activities; …misleading or persuading adversaries to opt for disadvantageous courses of action; …gives a means to gain operational advantage; and preserves C4I assets."[36] He also states that NSD is suited for the "…compliment of conventional elements of a broad deception, ...and the provisioning of a layer of protection to information within networks."[37] The former description of NSD is suited to "masking the extent and disposition of network activities, fabricating mock data networks, and creating the impression of authentic information with associated processes where none will actually occur."[38] The latter of these topics describes the "…provisioning of a layer of protection to information within networks, …to conceal the intent or shroud the information on a network or perhaps even cloak the true purpose for which that network is used."[39] Capt Erdie was quite clear that further work needs to occur in using NSD, in "…implementing deception techniques and deceptors specific to communications networks, such as feint or decoy networks."[40]

It is important to note that Captain Erdie is not the first to espouse the utility of deception in information networks. Dr. Fred Cohen wrote a 1998 paper titled "A Note on the Role of Deception In Information Protection", and Singapore Army Lieutenant Colonel Tan wrote a 2004 paper entitled "Confronting Cyberterroism with Cyber Deception". In both the Cohen and Tan works, there is much discussion of various defensive deception techniques, and how they can be used for the protection of cyber assets. These techniques are grouped per the scheme according to James Dunnigan and Albert Nofi "Victory and Deceit - Dirty Tricks at War", and are annotated below based on the relevancy to cyber tactical deception.

> **"Camouflage**
> **Noise injection:** Noise is injected in order to reduce the signal to noise ration and make compromise more difficult. Examples include the creation of deceptions involving false or misleading information, the induction of electrical, sonic, and other forms of noise to reduce the usability of emanations, and the creation of active noise-reducing barriers to eliminate external noises which might be used to cause speech input devices to take external commands or inputs. This form of camouflage has been very successful at making it more difficult for attackers to get a clear picture of the items being sought.
>
> **Lies**
> **Feeding false information:** False information is fed to attackers in order to inhibit the success of their attacks. Examples include: providing misleading information to cause foreign governments to spend money on useless lines of research, providing false information that will be easily detected by a potential purchaser of information so that the attacker will lose face, and the creation of honey pots, lightning rods, or similar target systems designed to be attractive targets and redirect attacks away from more sensitive systems."[41]

Also of note from Dr. Cohen, in his paper titled "The Use of Deception Techniques: Honeypots and Decoys", are the following properties of deceptions:

- "Deceptions increase the attacker's workload

- Deception allows defenders to better track attacks and respond before attackers succeed
- Deception exhausts attacker resources
- Deception increases the sophistication required for attack
- Deception increases attacker uncertainty"[42]

The works of these gentlemen provide the entry point for what AFSPC should do to protect its cyber resources. AFSPC should implement tactical deception in its computer networks to realize the benefits of NSD in the protection of information. Specifically, AFSPC should use enterprise wide traffic generation to implement and manage a deception protection campaign for Air Force network-based resources. This is different from a traditional honeypot or honeynet in that the goal is not to capture, collect, or learn about the attacks or the attackers by providing a vulnerability rich environment. The main purpose of this massive traffic generation scheme is to obfuscate the day-to-day traffic within USAF networks.

To implement such a campaign, AFSPC must take into account data collected from a study of the various types of networks belonging to the Air Force portion of the GIG. These data collections shall occur via the standard day model discussed earlier in this paper. Once these types of data are understood, they must then feed into an enterprise wide traffic generator, with many repeater generators at region or base level. This hierarchical architecture would allow updates at the "root level" of the Air Force enterprise to cascade down to the individual regions or bases. The traffic generation flows must also alternate in terms of services offered, ports opened, and types of operating systems available. The alternation scheme should be controlled at Air Force "root level", and change based on several factors. The logical organization for control of this operation is 24th Air Force. Additionally, referencing the cybermindedness

chapter from above, the minimizing of network traffic is key for this success. Limiting the amount of traffic and services will provide less avenues for attack, minimize the true traffic on the network, and allow for ease of flow of deception generated traffic.

The rotation for traffic generation deception should be based on a daily, weekly, and INFOCON basis. Implementing this would hamper the surveillance and reconnaissance capabilities of GIG intruders by increasing the workload of the potential attackers. In essence, the more clutter that exists, the more clutter that has to be sorted prior to launching an attack on the GIG. This tactic would implement the camouflage and lies portion of the Dunnigan and Nofi theory as well as all of the above-mentioned bullets concerning deception properties from the Cohen work. Again, an important distinction between this approach and that of a traditional honeypot or honeynet is the disinterest in capturing or collecting on the attacker. The traffic generator is simply a means of creating chaff to hide within while not providing a vulnerability rich environment.

To aid in clarification, a small scale example is called for. Say that a network contains 100 nodes. This network transmits privacy act information. Assume that the network is under reconnaissance by outsiders who are determining attack vectors to capture the information on this network. These attackers are using various weapons to determine any vulnerabilities that exist on the targets that are available. The "battlefield" is static and unchanging, thus making reconnaissance efforts easy for the attackers. On the contrary, if the same network were to employ tactical deception, the attackers would be faced with an ever changing battlefield, as the type of services offered, operating systems available, data transmitted, and ports opened/closed would all change on a random basis. Each of these factors would qualify as unique aspects to determine the random character of the network. Therefore the changes could happen by either

operating system, service, data transmitted, or ports while holding the other factors constant (ex. change operating system, yet hold, service, data transmitted, and ports stagnant); or one could vary two or more factors (ex. change operating system, service, data transmitted, and ports simultaneously). This type of dynamic environment would severely hamper the reconnaissance efforts of the 100-node network mentioned earlier, as the mapping of the battlefield would constantly be in a state of disarray. One can begin to understand the benefits of this rotation scheme for network randomization as the type and phase of conflict (major combat operations or irregular warfare) changes.

Ideas similar to this have been discussed prior, as per the Major Repik Air Force Institute of Technology paper entitled "Defeating Adversary Network Intelligence Efforts with Active Cyber Defense Techniques." In his paper, Major Repik suggests ideas such as Network Address Hopping ("…active defense tactic that dynamically changes a computer's network identity with the dual objective of hiding its real identity and confusing the attacker during reconnaissance")[43], Honeypots ("…designed to duplicate an application or system as closely as possible with the objective of deceiving intruders into interacting with them. All activity is monitored, logged, and captured. Additionally, they include features to limit their effectiveness as an attack platform if compromised.")[44], and Network Telescopes ("…sensor used to detect overt large-scale malicious activity…deployed in regions of routable, but unused IP address space (eg. Dark IP space) where legitimate traffic shouldn't appear.").[45] Major Repik also addresses the need for future work in the area in terms of using traffic generation to "increase the realism of honeynets by enabling them to mimic the 'emanations' of operational networks."[46] Furthermore, he suggests that "…accurate characterization of each network's 'emanations' would be key. These signatures would also likely evolve over time, so determining that rate of change and

periodically update them would be required. Though less robust, generic signatures could also be developed."[47] He then further states that research is needed to determine if characterizing or mimicking a network's signature if plausible and possible.[48] This speaks directly to the proposed establishing of a cyber standard network model, mentioned above. Additionally, this ties into this paper's assertion that each of these ideas is autonomous, yet when put together they are most effective.

What is suggested within this section of this paper is directly inline with the methodologies applied by both Chinese and Russian cyber doctrine, according to Timothy Thomas, author of "Nation-state Cyber Strategies: Examples from China and Russia". Both believe that it is beneficial to cause confusion on your enemy's behalf. The Chinese and Russians refer to information warfare as informationization. Chinese informationization doctrine includes:

1. "sabotaging the enemy's overall information operational structure
2. weakening the enemy's information fighting capacity
3. diverting an enemy's reconnaissance attempts and making sufficient preparations
4. giving the enemy a false impression while simultaneously launching a surprise information attack
5. making an enemy come up with a wrong judgment or take a wrong action."[49]

Furthermore, and key to the proposition of creating tactical deception within Air Force networks, Chinese military strategists use informationization doctrine as a means to "intimidate, employ perception management, and the employment of fictitious objects (such as fake networks and equipment in an information system) as part of a deception plan whose intent is to hide true reality."[50] Russian cyber doctrine is extremely close to that of the Chinese cyber doctrine. The

Russian viewpoint is stated more as perception management or reflexive control versus blatant deception. However it is important to note that both nation states, especially China, admit to the use of deception to hide true intent of cyber networks. The age-old adage of fighting fire with fire is appropriate here, as AFPSC would simply use deception to cloud the true purpose of its networks.

Although the tactics and even the title of this section are based on deception, it is important to note that tactical deception for cyber protection is more analogous to self-defense than traditional military deception. Tactical deception for protection of cyber resources should resemble using chaff and flare to protect a plane from an RF or IR missile.[51]

If engaged, fighter pilots do not have to seek permission to protect themselves from an impending missile attack. The decision, more accurately the responsibility, to protect rests with the operator of the weapon system and not with an outside source. Pilots employ the tactics, techniques, and procedures that they have been trained upon to protect crew and jet. Chaff is designed to deceive the incoming missile to by masking the radar cross section of the weapon system. The same concept is applied with the use of flares, except that the missile is made to believe that there is a better heat source than that of the jet in question.[52] Given that the sole purpose of these two types of self-protect measures is to deceive a hostile threat, it is allowable for network defenders to employ the same tactics in order to protect cyber resources from hostile threats.

Tactical deception in cyber networks is used to achieve information security. It is important however that the fake traffic not introduce any form of vulnerability into the network. An example would be the characterized traffic from a personnel systems network that transmits privacy information in the clear or has a well known vulnerability within the traffic flows of the

network. The availability of legitimate privacy act information would be unacceptable as part of a deception campaign, as real user data is presented to potential hackers. Additionally, even though the traffic is random and fake, presenting a well known vulnerability has the potential to provide the attacker with additional information as to the legitimacy of the traffic, or an attack vector on real hosts and traffic flows. It must not be lost that the purpose of the tactical deception campaign is to increase attacker workload by presenting a dynamic, agile, and flexible target, and not to learn about new attack patterns, tools, or the attackers themselves.

Conclusion

Others have written on the need for deception when dealing with cyber resources. Their work has mostly centered on the use of honeypots of honeynets to entice attackers into the network for active reconnaissance of the attackers. The goal of tactical deception for protection is to cause the confusion, fog, and friction that many war theorists have stated exists (Sun Tzu, Clausewitz, and Jomini to name a few). Conventional wisdom states that the hardest target to hit is a moving target. Randomized, realistic, characterized traffic generation for tactical protection would provide a decisive advantage for network operations.

ENDNOTES

[1] AURIMS, AFSPC Academic Year 2010 Topic: Cyberspace Protection
[2] AURIMS, AFSPC Academic Year 2010 Topic: Cyberspace Theory
[3] SAF/XC briefing, slide 15.
[4] Biddle, Rhetoric and Reality in Air Warfare, 33
[5] Ibid.,149.
[6] Ibid.
[7] Ibid., 148-149.
[8] SANS Institute email.
[9] Terrence O'Brien, "Study Finds Schools Lacking Cyber Security and Safety Education", 28 February 2010. http://www.switched.com/2010/02/28/study-finds-schools-lacking-cyber-security-and-safety-education/ (accessed 06 March 2010).
[10] National Cybersecurity Awareness Campaign Challenge, http://www.dhs.gov/files/cyber-awareness-campaign.shtm (accessed 06 March 2010).
[11] Ibid.
[12] The United States Air Force Blueprint for Cyberspace, 7.
[13] Ibid.
[14] Defense Contractor A, (Technical Manager), to the author, e-mail, 10 December 2009.
[15] Ibid.
[16] Elizabeth B. Lennon, "Testing Intrusion Detection Systems," iTL Bulletin (July 2003): 2, http://www.itl.nist.gov/lab/bulletns/bltnjul03.htm , (accessed 12 December 2009).
[17] Major Sylvester (C-17 pilot and Air Command and Staff College student), various interviews by author, November - December 2009.
[18] DOD Dictionary of Military Terms, s.v. "cyberspace", http://www.dtic.mil/doctrine/dod_dictionary/data/c/01469.html (accessed 12 December 2009).
[19] National Test Pilot School, Introduction to Performance and Flying Qualities Flight Testing, (December 2005), 4.1
[20] National Oceanic and Atmospheric Administration, U.S. Standard Atmosphere, 1976, (Washington D.C.: Government Printing Office, 1976), 3–14, http://www.pdas.com/refs/us76.pdf , (accessed 12 December 2009).
[21] Lieutenant Colonel Bailey, (Air Force Research Labs and Flight Test Engineer), to author, e-mail, 03 December 2009.
[22] Major Bonner (Flight Test Engineer and Air Command and Staff College student), interview by author, 04 December 2009.
[23] National Test Pilot School, Introduction to Performance and Flying Qualities Flight Testing, (December 2005), 4.4 - 4.6.
[24] National Oceanic and Atmospheric Administration, U.S. Standard Atmosphere, 1976, (Washington D.C.: Government Printing Office, 1976), 15, http://www.pdas.com/refs/us76.pdf , (accessed 12 December 2009).
[25] Major Bonner (Flight Test Engineer and Air Command and Staff College student), interview by author, 04 December 2009.
[26] Defense Contractor B, (Senior Security Engineer), interview by author, 01 December 2009.
[27] Defense Contractor A, (Technical Manager), interview by author, 01 December 2009.
[28] Defense Contractor A, (Technical Manager), to the author, e-mail, 10 December 2009.
[29] International Civil Aviation Organization Standard Atmosphere Model and U.S. Standard Atmosphere, 1976
[30] National Oceanic and Atmospheric Administration, U.S. Standard Atmosphere, 1976, (Washington D.C.: Government Printing Office, 1976), 15, http://www.pdas.com/refs/us76.pdf , (accessed 12 December 2009).
[31] Repik, Defeating Adversary Network, 50.
[32] Erdie, NETWORK-CENTRIC STRATEGIC-LEVEL DECEPTION, 11.

[33] Ibid, 1.
[34] Ibid, 1, 6.
[35] Ibid, 3.
[36] Ibid, 2-3.
[37] Ibid, 11.
[38] Ibid, 11.
[39] Ibid, 11.
[40] Ibid, 32.
[41] Cohen, A Note on the Role of Deception in Information Protection, 1.
[42] Cohen, The Use of Deception Techniques: Honeypots and Decoys, 9.
[43] Repik, 24.
[44] Ibid, 43.
[45] Ibid, 46.
[46] Ibid, 50.
[47] Ibid, 50.
[48] Ibid, 50.
[49] Thomas, Nation-state Cyber Strategies: Examples from China and Russia, 470-471.
[50] Ibid, 472.
[51] Cohen, The Use of Deception Techniques: Honeypots and Decoys, 2.
[52] Ibid, 2.

BIBLIOGRAPHY

Air University Research Information Management System, Air Force Space Command Academic Year 2010 Topic: Cyberspace Protection . https://www.afresearch.org/ subject Cyberspace Protection.

Air University Research Information Management System, Air Force Space Command, AFSPC Academic Year 2010 Topic: Cyberspace Theory. https://www.afresearch.org/ subject Cyberspace Theory.

Bailey, Lieutenant Colonel (USAF). "Help with Research Topic", 02 December 2009. Personal email (03 December 2009).

Biddle, Tami Davis. Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945. Princeton, NJ: Princeton University, Press, 2002.

Bonner, Major (USAF). Interview by author, 04 December 2009.

Builder, Carl H. The Masks of War: American Military Styles in Strategy and Analysis. Baltimore, MD: The Johns Hopkins University Press, 1989.

Cohen, Fred. A Note on the Role of Deception in Information Protection. © 1998. http://all.net/journal/deception/deception.html (accessed 28 January 2010).

Cohen, Fred. A Mathematical Structure of Simple Defensive Network Deceptions. © 1999. http://all.net/journal/deception/mathdeception/mathdeception.html#footnote-1 .

Cohen, Fred. The Use of Deception Techniques: Honeypots and Decoys. http://all.net/journal/deception/Deception_Techniques_.pdf.

Defense Contractor A. Interview by author, 01 December 2009.

Defense Contractor A. "Review of Research Topic", 10 December 2009. Personal email (10 December 2009).

Defense Contractor B. Interview by author, 01 December 2009.

DOD Dictionary of Military Terms, s.v. "cyberspace", http://www.dtic.mil/doctrine/dod_dictionary/data/c/01469.html (accessed 12 December 2009).

Erdie, Captain (USMC). "NETWORK-CENTRIC STRATEGIC-LEVEL DECEPTION," Naval Post Graduate School (September 2004).

Home Network Security (Non-Technical), http://www.us-cert.gov/reading_room/home-network-security/#IV-A-4 (accessed 06 March 2010).

Lennon, Elizabeth B. "Testing Intrusion Detection Systems," itl Bulletin (July 2003), http://www.itls.nist.gov/lab/bulletns/bltnjul03.htm (accessed 12 December 2009).

National Cybersecurity Awareness Campaign Challenge, http://www.dhs.gov/files/cyber-awareness-campaign.shtm (accessed 06 March 2010).

National Oceanic and Atmospheric Administration, U.S. Standard Atmosphere, 1976, (Washington D.C.: Government Printing Office, 1976), http://www.pdas.com/refs/us76.pdf , (accessed 12 December 2009).

National Test Pilot School, Introduction to Performance and Flying Qualities Flight Testing, (December 2005).

O'Brien, Terrence. Study Finds Schools Lacking Cyber Security and Safety Education, 28 February 2010. http://www.switched.com/2010/02/28/study-finds-schools-lacking-cyber-security-and-safety-education/ (accessed 06 March 2010).

Repik, Major. Defeating Adversary Network Intelligence Efforts With Active Cyber Defense Techniques

"SAF/XC Update AFCEA Luncheon". Briefing, by Lieutenant General Lord, Chief Warfighting Integration and Chief Information Officer. 18 September 2009.
SANS Institute email, SANS Newsbites Volume 12 Number 15 23 February 2010. Subscription email (23 February 2010).
Sylvester, Major. Interview by author, November - December 2009.
Tan, Lt Col (Singapore Army). CONFRONTING CYBERTERROISM WITH CYBER DECEPTION. December 2003.
The United States Air Force Blueprint for Cyberspace. November 02, 2009.